18th International Command and Control Research and Technology Symposium

"C2 in Underdeveloped, Degraded and Denied Operational Environments"

Title of Paper

Tactical Networking Requirements for Digital Command and Control

Topic 8

Networks and Networking

Authors

Lieutenant Colonel Michael M. Cho, USMC

Major Kurt M. Gall, USMC

Major Jeffrey L. Hammond, USMC

Major James M. Robinson, USMC

Major Henry R. Salmans III, USMC (Retired)

Point of Contact

Major Henry R. Salmans III (USMC, Retired) of Computer Sciences Corporation

Technology Services Organization, Programs & Resources, HQMC

Kansas City Information Technology Center (KCITC)

2306 E. Bannister Road

Kansas City, MO 64131-3088

Direct: (785) 840-7066

Henry.Salmans.ctr@mcw.usmc.mil

Report Documentation Page

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JUN 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**
4. TITLE AND SUBTITLE **Tactical Networking Requirements for Digital Command and Control**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Computer Sciences Corporation,Technology Services Organization, Programs & Resources, HQMC,2306 E. Bannister Road,Kansas City,MO,64131-3088**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES **Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 19-21 June, 2013 in Alexandria, VA.**		

14. ABSTRACT

Operating within a dynamic, counterinsurgency (COIN) environment has exponentially increased the need for digitization of Command and Control. Within that COIN environment, acetate overlays and hand written ?yellow canaries? are no longer effective means to manage volumes of information needed today to convey strategic context, develop situational awareness, and make quick-turn tactical decisions that could have operational and strategic impacts. The modern tactical commander now manages a breadth and depth of information comparable to what theater commanders and their supporting staffs were responsible. On the modern battlefield, access to information is key to maintain tactical effectiveness and agility. The Marine Corps has reached a point in the maturation of information technology where ?stand alone? computing is no longer an option: the warfighter must be networked at all times and at all locations. Given ten years? experience operating in COIN, what are the realistic networking requirements for high tempo combined arms offensive operations that require a unit to maneuver 400 miles in ten days while fighting the enemy? The challenge is to understand the type of warfare and tailor the networking capacity to fit the needs of the commander. Continuing to provide the significant level of network connectivity that commanders have become accustomed to within the longstanding COIN environments of Afghanistan and Iraq creates challenges for command, control, communications, and computer (C4) planners. In future operations where forces are highly mobile and disaggregated current C4 systems will not be able to provide the same levels of network connectivity as experienced in the COIN environment. This paper will: (1) describe the strengths and vulnerabilities of Digital Command and Control; (2) elaborate the operational requirements for tactical network connectivity as part of the modern battlefield geometry across the spectrum of conflict that must be identified, procured, or defended, and (3) propose a framework for developing tactical networking.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**19**	

Abstract

Operating within a dynamic, counterinsurgency (COIN) environment has exponentially increased the need for digitization of Command and Control. Within that COIN environment, acetate overlays and hand written "yellow canaries" are no longer effective means to manage volumes of information needed today to convey strategic context, develop situational awareness, and make quick-turn tactical decisions that could have operational and strategic impacts. The modern tactical commander now manages a breadth and depth of information comparable to what theater commanders and their supporting staffs were responsible. On the modern battlefield, access to information is key to maintain tactical effectiveness and agility. The Marine Corps has reached a point in the maturation of information technology where "stand alone" computing is no longer an option: the warfighter must be networked at all times and at all locations. Given ten years' experience operating in COIN, what are the realistic networking requirements for high tempo combined arms offensive operations that require a unit to maneuver 400 miles in ten days while fighting the enemy? The challenge is to understand the type of warfare and tailor the networking capacity to fit the needs of the commander. Continuing to provide the significant level of network connectivity that commanders have become accustomed to within the longstanding COIN environments of Afghanistan and Iraq creates challenges for command, control, communications, and computer (C4) planners. In future operations where forces are highly mobile and disaggregated current C4 systems will not be able to provide the same levels of network connectivity as experienced in the COIN environment.

This paper will: (1) describe the strengths and vulnerabilities of Digital Command and Control; (2) elaborate the operational requirements for tactical network connectivity as part of the modern battlefield geometry across the spectrum of conflict that must be identified, procured, or defended, and (3) propose a framework for developing tactical networking.

Disclaimer

This paper presents the views of the authors and does not represent any official position within the Department of Defense.

Introduction

The gap between digital Command and Control and the underlying network infrastructure that supports it is worthy of consideration. Recent operational experience in a counterinsurgency (COIN) environment has resulted in a demand and expectation by tactical commanders for continuous network connectivity to enable modern Command and Control. However, the ability to provide continuous network connectivity will be problematic for future expeditionary environments. In contrast with recent counterinsurgency environments, austere environments categorize future warfare and do not allow for a gradual buildup of telecommunications infrastructure.

The United States military's collective history of operating within a dynamic, counterinsurgency environment has exponentially increased the need for the digitization of Command and Control. Within that COIN environment, acetate overlays and hand written "yellow canaries" are no longer effective's means to manage the volumes of information needed today to convey strategic context, develop situational awareness, and make quick-turn tactical decisions that could have operational and strategic impacts.

The modern tactical commander now manages a breadth and depth of information that was previously reserved for theater commanders and their supporting staff. On the modern battlefield, access to information is key to maintain tactical effectiveness and agility. The Marine Corps has reached a point in the maturation of information technology where "stand alone" computing is no longer an option: the warfighter must be networked at all times and at all locations. Given ten years' experience operating in the COIN environment, what are the realistic networking requirements for high tempo combined arms offensive operations that require a unit to maneuver 400 miles in ten days while fighting the enemy? The challenge is to understand the fight we are in and tailor the networking capacity to fit the needs of the commander. Providing the significant level of network connectivity commanders have become accustomed to within the longstanding COIN environments of Afghanistan and Iraq is not possible in emerging austere threat environments with command, control, communications and computer (C4) systems currently available to warfighter.

The concept of what is to be expected by an expanded C2 capability was expressed recently by Brigadier General Kevin J. Nally[1] as Networking On The Move (NOTM). The implication for tactical networking is for the Marine Corps to move "everything over IP [Internet protocol]" and in effect, "fill the gap of providing an on-the-move command and control capability that reaches over the horizon."

This paper focuses the discussion on tactical commanders at the company and below levels. While Command and Control and network connectivity has evolved for all levels of command, it is at the company and below levels where tactical commanders have most been inundated with information for command and control; it is also at these levels where current organic equipment and personnel are inadequate to support modern Command and Control in future operations.

Command and Control

Principles of Command and Control (C2)

A doctrinal overview of Marine Corps C2 points to the expeditionary and maneuver warfare proclivities outlined in numerous publications. The challenge for today's commanders lies in establishing the balance between what is available, what is possible, and what is necessary in regards to the information technology that supports the C2 of Marine expeditionary operations. After operating within a counterinsurgency environment for over ten years, the capabilities of information technology have taken a front seat effectively dictating how and in what format C2 will be conducted. The blur between C2 and C4 (Command, Control, Communications, and Computers) within Marine units has become nearly imperceptible, presenting serious doctrinal challenges. To alleviate the bandwidth requirements necessary to operate the myriad of applications and information technology, the Marine Corps has spent the last ten years procuring tactical radio assets that provide enough bandwidth to match the requirement by the systems being fielding. What the Marine Corps has done is subscribed to a finite example of Moore's Law where information technology requirements are expanding exponentially. Simultaneously, the Marine Corps is pushing the envelope for what is technologically possible with the very radio assets being procured.

[1] Brigadier General Kevin J. Nally is the Director, C4/CIO of the Marine Corps, and the Deputy Commander, Marine Forces Cyber Command.

The seminal publication, Marine Corps Doctrinal Publication 1 – Warfighting, outlines how the Marine Corps understands the nature and theory of war and subsequently how it prepares and conducts itself in war. Beyond Clausewitz, MCDP-1 provides a relevant roadmap for Marines to understand how the organization sees itself in relation to the rest of the defense establishment and provides a roadmap for commanders and leaders to prepare their organizations and Marines for war. "First and foremost, *in order to generate the tempo of operations we desire and to best cope with the uncertainty, disorder, and fluidity of combat, command and control must be decentralized*. That is, subordinate commanders must make decisions on their own initiative, based on their understanding of their senior's intent, rather than passing information up the chain of command and waiting for the decision to be passed down."[2] Furthermore, it is a tenant of well-formed Command and Control to be able to Command and Control assigned forces in the absence of communications to higher. Anything less results in a failed Command and Control architecture.

In this context, the commander's challenge is to effectively generate enough of a C4 apparatus without stymieing a subordinate leader's initiative. "How much and of what kind of C4 is necessary" is something that has not been answered effectively and has arguably been significantly distorted given the unique dynamics of the various conflicts the Marine Corps has participated in during the last ten years. Technological innovations over the past twenty years have provided a significant sensor to shooter time reduction while significantly increasing the lethality and accuracy of weapons systems. The intelligence capabilities built from technological advancements in unmanned reconnaissance, correlation database structures, and geospatial assets are phenomenal. The raw processing power of integrated circuitry has exponentially evolved enabling data generation that can rapidly overwhelm the system left unmanaged. Likewise, situational awareness as defined by knowing where an individual on the battlefield is, his respective senior and subordinate units as well as adjacent organizations, and the extremely detailed topographic map are beyond anything that just a previous generation of Marines could have ever hoped for.

---

[2] *Marine Corps Doctrinal Publications MCPD 1* (Washington, DC: Department of the Navy, Headquarters United States Marine Corps, 1997), 78.

But are all the technological advances aiding in the generation of tempo relative to the enemy and assisting commanders at all levels cope with the fog and friction of war in an expeditionary environment? The question of how much and in what form C4 is needed at all levels should be fairly straightforward to answer. The proliferation and ad hoc nature of new technology integration exacerbates C2 maturation when organizations forgo sound principles tied to actual requirements. The commercial sector through the ever evolving introduction of cutting edge technology and innovation drives the procurement cycle of military C4 systems. Marines accustomed to purchasing new computers, mobile phones, and electronic devices for personal use because of largely novel improvements have transferred that expectation of perceived innovation onto military C4 structures. The unjustified need to have a newer, faster, and implicitly better piece of technology has created a fetish in the Marine Corps for an ever expanding C4 capability. This phenomenon is unsupportable for rapid decision making and much like civilians, the Marine Corps faces a danger, which if gone unchecked, will result in a combat leader constantly checking his C4 device on the battlefield and consequently failing to maintain situational awareness of the fight around him. The result may be the convex of the intent in providing the innovation.

To proceed, the Marine Corps must take stock of the current situation of C4 architecture in direct relation to what is necessary for effective C2 across a complex and expeditionary battlefield at all levels of the Marine Air-Ground Task Force (MAGTF). What C4 has been used effectively in support of counterinsurgency warfare needs to be analyzed in detail to determine where scarce resources should be placed to reinforce success. Simultaneously, an analysis of other scenarios of conflict across the spectrum of violence and austerity must be provided. By comparing what has been successful with what is expected in the future, an effective road map can be drawn that will plot a responsible course from now into the foreseeable future. That map must always keep in mind the essence of war as defined in MCDP-1; "The very essence of war as a clash between opposed wills creates friction. In this dynamic environment of interacting forces, friction abounds."[3]

---

[3] *Marine Corps Doctrinal Publications MCPD 1* (Washington, DC: Department of the Navy, Headquarters United States Marine Corps, 1997), 5.

The Digitization of Command and Control

Traditionally, technical limits constrained the span within which information could be shared. Rather than information being shared, information was pushed up to higher echelons for collection and processing. The C2 system on a general system might be quite robust, but at the tactical level the C2 system was a result of information directly gathered from the commander's eyes and ears.

The digital revolution has had a corresponding impact on the nature of C2. The ability to digitize information into bits, readily disseminate that information over data networks, and process that information with computer systems has shifted the C2 system from a highly centralized to a decentralized model. The Marine Corps has reached a point where there is no technical limitation to how, where, and when information is shared, with the only restriction being the resourcing of technology to implement throughout the battlefield. However, the point is that technology currently exists to enable the lowest tactical commander to access the same information and replicate the C2 system of the highest command echelons.

Within the Marine Corps, doctrinally the battalion was considered the lowest level of command with an inherent C2 system. Commands and platoons were extensions of the battalions C2 system. However, recent operations have demonstrated C2 systems being employed at the company and platoon level, where people, processes, information, and technology are implemented to enable the tactical commander to assess the situation, make decisions, and evaluate the execution of his decisions. America's Special Forces have provided unique opportunities to observe every minute detail of a battle or operation taking place from thousands of miles away. While this may have a positive impact on strategic level operations, oftentimes commanders at the Company and below level are threatened by the real, not perceived, threat that they operate under a microscope where leadership and ingenuity are replaced by micromanagement and second guessing by higher echelon commanders. This example is but one of many where decentralized leadership has become centralized to the detriment of basic Marine Corps warfighting principles

Strengths and Vulnerabilities

The digitization of C2, or digital C2, has not changed the fundamental principles of C2, but has certainly changed the character of C2 by enabling lower levels of echelon to execute C2, to decentralize operational responsibilities and authorities, and allow smaller formations to operate on increasingly larger areas of battlespace. Digital C2 is a necessity on the modern battlefield where a high degree of situational awareness is required to maintain the quick reaction time to effectively fight.

However, this has created an inherent vulnerability in that digital C2 is dependent on the supporting technology. This same level of C2 simply cannot be replicated with legacy analog systems of paper messaging and acetate map overlays. Tactical commanders have become steeped with digital C2, expecting the full capabilities of digital C2 in order to accomplish their missions and therefore they cannot effectively fight in the absence of C2. Rather than advocate for the ability to fight without digital C2 capabilities, the way forward is to develop the capabilities to ensure digital C2 given the realities of modern military operations.

Data Network Infrastructure

Digital C2 Capacity

The key to digital C2 is the data network infrastructure capable of passing the large amounts of information shared on the modern battlefield. Network infrastructure is the means to pass data traffic between applications which are translated to information for the commander to assess the tactical situation, make decisions, and measure the execution of those decisions. Robust and readily available network infrastructure is taken for granted in fixed garrison environments, and has become the norm in COIN operational environments. However, military planners and capability developers must acknowledge the realities of digital C2 and the growing need for readily available, secure, reliable, and robust data networks to support digital C2 within the constraints of mobile and ad-hoc tactical networking.

Network Technology

There are numerous technologies capable of providing robust data network infrastructures. The most efficient and secure are wired infrastructures, although these require the most time to install

and are the least mobile. Forces operating from a predominantly fixed base allow for a gradual buildup of wired infrastructure. The challenge ahead is the expeditionary.

Satellite communications have the benefits of enabling worldwide coverage and autonomy. Bypassing local infrastructure also has some inherent strength regarding cyber vulnerabilities. Cost effective high-speed data networks required for digital C2 are only available through larger, heavier satellite equipment and are not suitable for highly mobile ground forces.

Wireless communications refers to communications between two land based nodes. Typically this mode of communications is for voice-based radio. However, new waveforms and improved technology have enabled vehicle and man-portable radios to effectively pass data across the battlefield. Furthermore, emerging technologies with network management allow for self-forming mesh networks enabling data traffic to hop from radio to radio until reaching the intended destination. The introduction of this type of mesh network on the battlefield, in absentia of a dedicated network manager, allows maneuver units to maintain tempo, without the need for dedicated retransmission sites. Through effective employment of wide-band, mesh networking radios, the Marine Corps can now effectively leap frog “advantaged nodes” to high ground without having to employ fixed sites, thereby increasing tempo, while simultaneously providing necessary throughput for combat systems.

Network Management

Another complexity that arises with digital C2 is the need to actively monitor and manage the data network. The data network in essence requires its own C2 capacity to monitor the capacity of the network, make decisions on changes to implement, and monitor the execution of those changes. Data network management is dynamic with the capacity of the network constantly in flux due to human error, human malicious activity, technical failures, and even natural disasters. This is especially true for military operations where tactical nodes routinely become established and de-established. One of the critical capabilities the authors have seen firsthand is the network management of the wideband networking technologies provided for with Advanced Networking

Wideband Waveform (ANW2) in the AN/PRC-117G Wideband Tactical Radio[4]. In a dynamic battlefield, where units typical jump their forwards and their mains multiple times in a single day, there is insufficient time to establish fixed retransmission sites, while still maintaining the tempo of the battle. To mitigate this, the Marine Corps must utilize technologies such as the Simple Network Monitoring Protocol (SNMP) to monitor the health of the network. The absence of monitoring dictates that the communicator maintain a reactive posture where a forward or edge unit to the flanks may out-pace or out-distance its next available node in a wideband mesh-network. The technology exists today for a Marine with a laptop to monitor the waveform ID status and signal strength of each node within his network. A practical evolution would be to develop a graphical user interface or application to enable this capability that is already resident in the AN/PRC-117G. To do so would ensure the communications officer is proactive in maintaining network health, improve the tempo of the battle, and allow the commander to press the attack. Along this paradigm of moving more C2 capability down to lower tactical echelons requires a comprehensive approach to fighting within a single integrated global network.

Data Networking on the Modern Battlefield

COIN Experience

The Marine Corps has been involved in the Global War on Terrorism for over a decade. The Marine Corps' involvement has been primary focused on COIN operations which require a continuous presence and relationships with the local population. Marine Corps data networks began with expeditionary military equipment with constrained capabilities, and has gradually evolved to fixed infrastructure using commercial equipment to provide data networking capabilities that provide tactical commanders with a quality of information sharing that is on par with what can be found in garrison. Many fixed bases in Iraq and Afghanistan are characterized by permanently installed, in-ground fiber optic infrastructure and large dedicated facilities to house all the networking, data server, and information assurance equipment. One capability that is lacking in the current architecture is that of aerial layer communications retransmission. For

[4] The AN/PRC-117G is Joint Tactical Radio System (JTRS) Certified for procurement or operations in a DoD or Service's network architecture.

the past twenty years, the Marine Corps has delved into the Unmanned Aerial Systems world with a primary focus on Intelligence, Surveillance and Reconnaissance (ISR). The missing link in this capability is aerial layer retransmission where every UAS platform is capable of retransmission of wideband radios transmission. It is naïve to think that future conflicts will enable friendly forces to capitalize on traditional retransmission sites located on logical high ground. Each of the Marine Corps operational plans have distinct attack zones that are logical to where enemies can foresee them; therefore, it follows that they also recognize the high ground, and have pre-planned targets on this ground. There are two venues to mitigate this threat. First, employ manned aircraft equipped with communications suites to provide continuous coverage of communications across the battlefield. Second, harness the plethora of UAS assets available to the modern battlefield down to the company level to ensure aerial retransmission is available to them as needed by the echelon of command. Black side RF technology exists today to extend networks from a platoon or company sized UAS to close communications gaps in echelon from lower to higher.

Marine Expeditionary Requirements

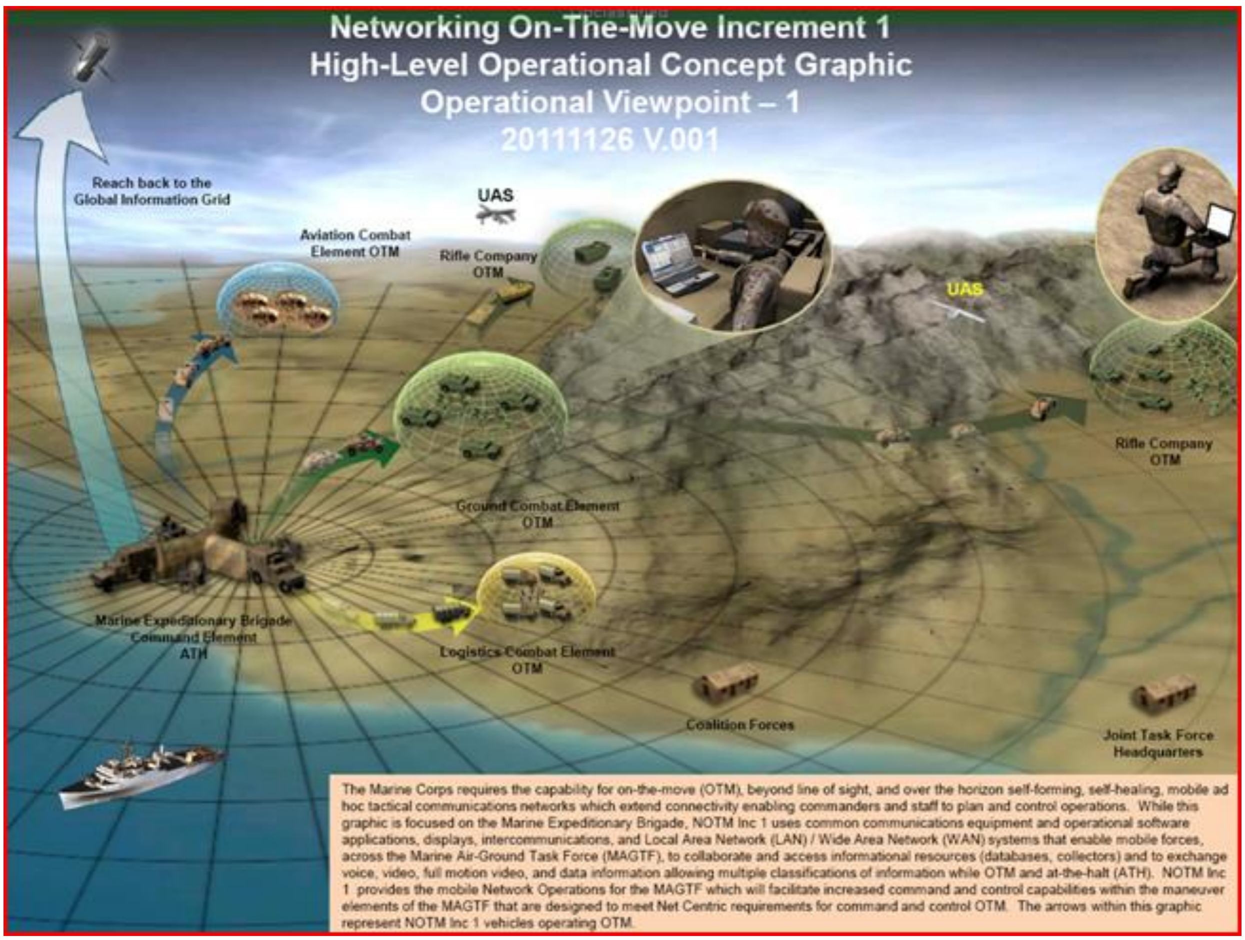
Tactical commanders at all levels are accustomed to high-capacity digital C2, but traditional Marine Expeditionary operations will not benefit from a long buildup in the infrastructure found in COIN environments. The current vulnerability is an expectation for immediate access, on-the-move digital C2 that is not realistic with today’s C4 systems. Simply stated, digital C2 for expeditionary operations does not exist to the extent that tactical commanders have become accustomed to while fighting in a COIN environment.

For Marine expeditionary operations, tactical commanders will expect to have access to C2 systems and vast amounts of data to understand the tactical situation, make decisions, and monitor the execution of those decisions. The continuous flow of information to commanders can be both beneficial, as well as harmful. Coalition Joint Task Force 58, which led the initial Marine involvement into Afghanistan in 2001, prided itself in the decentralized command and control, with mission type orders, to two separate Marine Expeditionary Unit (MEU) command elements. There was oversight, but there was not a rapid introduction of information during the execution cycle of the operations the Task Force was assigned. This autonomy of command and execution of commander’s intent served both the MEU Commands, as well as the CTF command

element, well and resulted in resounding success. However, current support to the tactical commander only allows for access to C2 systems during the planning phase, with C2 systems for the remainder of the operation being constrained to Single Channel Radio. What is needed is the full range of digital C2 capabilities associated with the COIN environment available to tactical commanders conducting expeditionary operations.

Not only will Marines expect to have unfettered access to C2 information, there will be an increasing demand to communicate with more nodes within the C2 network. No longer is communications with higher, adjacent, and subordinate headquarters sufficient for the tactical commander. Future Marine operations will mirror Special Operations during the initial volleys of combat, such as in Afghanistan, where operators on horseback had access to national intelligence assets and airborne strike capabilities.

The current initiative to provide as much capability to the tactical edge is presented below.



Future

Marines must be prepared to deploy to any region of the world to fight in all types of terrain against a determined and capable foe. The trend is for Marines to fight in smaller units given a larger span of responsibilities, all while being even more removed from headquarters support. The key to enabling this will be digital C2 with underlying data network capabilities that are quick to establish, able to stay connected while on the move, and able to be self-managed. Even if the Marine Corps explores the current reliance on Ku commercial satellite communications, it is not feasible during engagement to expect this to be as proliferated as it is today. Unclassified reports of enemy capabilities show that jamming of Ku and Ka satellite communications bands is prevalent throughout the world. The limited number of X band terminals creates a dilemma in the attempt to "feed the beast" with unfettered access to C2 systems and digital C2 information. The Marine Corps would be naïve to think that both wideband HF and wideband Terrestrial communications do not play an important role in future capabilities to a satellite communications denied Marine Corps. Each of these capabilities requires the communications officer to be well informed as to the network costs of the applications being provided to commanders in any environment. The expectation of data heavy instances of SharePoint, Command Post of the Future (CPOF), and 5 megabyte PowerPoint slides shows is not practical when C4 architecture is exacerbated or disrupted. Scaling from the Deployable KU band Earth Terminal (DKET) throughput down to the ANW2 networks and wideband HF capabilities shows exponential reductions in bandwidth, as well as an inability to provide to the commander the aforementioned C2 applications. It is reasonable to expect that in the event Ku satellite communications were in fact jammed, the communications officer will have to be prepared to identify to commanders what his most costly applications are in terms of bandwidth, and present viable courses of action for available terrestrial assets to still perform command and control functions.

Understanding Digital C2 Capacity

Framework

Regardless of how the Marine Corps envisions the future battle space commanders will expect a level of assurance that they will continue to have digital C2. As of February, 2013, the Marine Corps has begun its fielding of the Networking on the Move (NOTM) capability to I Marine

Expeditionary Force (I MEF). This initial fielding consists of five Point of Presence (POP) vehicles, and ten Staff Vehicle Kits (SVK's) where each POP consists of a Ku On the Move (OTM) capability, two AN/PRC-117G radios capable of wideband ANW2 radios, Fortress Wireless, Talon Cards, inertial GPS navigation, VideoScouts, and three network enclaves. This capability will prove out the advanced offering of C2 digitization to commanders who will utilize this platform to tie in existing ANW2 capabilities to form a greater networked battlefield.

I MEF's experience in Operation Iraqi Freedom showed that a networked battlefield was a necessity for a modern battlefield. With a rapid push of 40,000 Marines over a ninety day period and 400 miles, the information exchange requirements outpaced the capability of available C4 systems architecture in 2003. There has been an increasing thirst for C2 digitization, in large part resultant from the spoiling factor of commercialized networks in the later years of the war in Iraq and now in Afghanistan. I MEF plans to utilize NOTM to maintain a minimum of 2MB of throughput up and 4MB of bandwidth down to the POP. This translates to the ability to fully utilize all virtualized applications contained on the three enclave network stack and horizontally share this information across the battalions, and vertically with the regiments utilizing the 54MB transmission pipe of the Fortress Wireless. If out of range of this scales to the 1-3MB capacity of the ANW2 network. With each of these transmission systems, including ANW2 at the lower tactical internet, the MEF will be fully capable of running all of its critical C2 applications. Intelligence, Surveillance and Reconnaissance (ISR) video downlink capability will ensure that the maneuver units of I MEF are capable of not only receiving accurate full-motion video of enemy targets and troops, but also of exploiting the same to keep the enemy off balance. With the fielding of an additional 40 ANW2 capable radios to each Infantry battalion the MEF will enjoy a robust terrestrial network, with sufficient bandwidth available to maintain an advantaged tempo over the adversary's. The goal is a net-centric battlefield where there does not exist a requirement to establish a conventional Combat Operations Center (COC), but only a requirement to maintain the same capability provided by this large equipment set with NOTM, a couple of 305 tents, fold out tables and chairs. The net impact to the MAGTF will be a network that is always in a "hot start" where a field expedient COC can be established in a matter of 10-15 minutes versus 2-5 hours. Additionally, the logistics footprint will be greatly reduced during Phase 1-3 of combat operations due in large part to abstaining from the requirement to bring two 7-ton's and multiple HMMWV's worth of equipment in the form of tents, tables, chairs, and the

robust Operational Trailer and components of a traditionally COC. Through the capability of NOTM, commanders will have a never before seen network, by any army in history. This network will be resilient to GPS jamming and spoofing, redundant in transmission capability, and capable of performing all required C2 applications.

While NOTM may seem like the desired end-state for Marine Corps battlefield networks, it is but a step in the right direction; one which must be built upon. Commanders must be weary of demanding the information technology that they received in Operation Enduring Freedom, and Operation Iraqi Freedom, with their mature networks and commercialized capabilities. Extensive bandwidth analysis of existing and emerging C2 systems is required to know how much each system costs us on any given tactical network. Further, detailed examination is required to ensure that Headquarters Marine Corps has a true appreciation for what the desires are of its commanders at battalion and below.

Requirements

A simple answer to future C4 challenges is to push out greater bandwidth on the battlefield. However, this approach fails to take into account the overall requirement for expeditionary forces to be ready, mobile, and self-supporting. C4 systems that are too heavy, complex, or delicate become a burden to the tactical force.

C4 capability developers will need a better understanding of the operational requirements for digital C2. The requirements analysis may indicate that what was experienced in a COIN environment greatly exceeds our doctrinal C2 requirements. The tactical commander must have enough information to quickly assess the situation, make decisions, issue orders, and monitor execution. However, too much information becomes a burden of analysis that potentially cripples tactical C2.

C4 requirements must assess and integrate how C4 systems are implemented and managed in an expeditionary environment. Another characteristic of the recent COIN experience has been the piece meal approach of systems fielding to rapidly field capabilities in response to critical deficiencies. This approach proved to be successful in an environment with an established telecommunications and logistical support network, but could be counterproductive in an expeditionary environment.

Conclusion

This paper attempted to highlight a gap between modern C2 requirements and existing C4 systems. This gap is less apparent in the current COIN environment where the telecommunications infrastructure has benefited from a long, gradual buildup. However, this gap is quite severe when looking at the tactical commander's C2 requirements in a true expeditionary environment.

The Marine Corps is addressing this gap with the Networking on the Move (NOTM) capability set. This effort begins to address the C4 requirements for expeditionary operations, but will not meet the standard of network connectivity that has been set through recent experience in the COIN environment. Continuous doctrinal review, requirements analysis, and systems development will be needed to ensure that the tactical commander is able to effectively C2 his forces on the modern battlefield.

Bibliography

ABI Research (2013). Cyber-attacks Against Oil & Gas Infrastructure to Drive $1.87 Billion in Cybersecurity Spending by 2018Retrieved from http://www.abiresearch.com/press/cyber-attacks-against-oil-gas-infrastructure-to-dr

Ackerman, Robert K. "Army Networking Technologies Change on the Fly." AFCEA. April 2008. Accessed February 05, 2013. http://www.afcea.org/content/?q=node/1552

Ackerman, Robert K. "Land Warfighter Enters New Networking Realm." AFCEA. March 2012. Accessed February 05, 2013. http://www.afcea.org/content/?q=node/2902

Ackerman, Robert K. "Technologists Plan Tactical Future." AFCEA. November 2001. Accessed February 05, 2013. http://www.afcea.org/content/?q=node/474

Avenetti, Q. (2005). Enhanced target acquisition platoon concept. Marine Corps Gazette, 89(6), 18-22.

Cacas, Max. "Corps Command and Control on the Move." AFCEA. March 2012. Accessed February 05, 2013. http://www.afcea.org/content/?q=node/2893

Cacas, M. (2012). Marines Go Back to the Amphibious Future. Signal Online. Retrieved from http://www.afcea.org/content/?q=node/2893

Defense Industry Daily Staff. "The US Military's DTCS Netted Iridium Program." Defense Industry Daily RSS News. March 11, 2011. Accessed February 05, 2013. http://www.defenseindustrydaily.com/217M-for-Phase-II-of-Netted-Iridium-Program-05483/

Department of the Navy, Program Executive Officer, Command, control, Communications, Computers and Intelligence (2012). Memorandum: PEO C4I Annual Acquisition Requirements for Science and Technology.

“EBU condemns Middle Eastern Satellite Jamming” Originally appeared in TV Technology. Radio World. 22 October 2012. Accessed February 06, 2013. http://www.rwonline.com/article/ebu-condemns-middle-eastern-satellite-jamming/216034

Ghourly, Scott R. "Company Command Post Initiative." ARMY Magazine, March 2012, 61-68. Accessed February 5, 2013. http://www.ausa.org/publications/armymagazine/archive/2012/03/Pages/default.aspx

Hamilton, S. R., Smith, R. L., & McCleary, M. C. (2008). Tactical persistent surveillance. Military Intelligence Professional Bulletin, 34(3), 7-18. Retrieved from http://www.fas.org/irp/agency/army/mipb/2008_03.pdf

Hansen, E. G. (2005). Digital command and control . . . just do it! Marine Corps Gazette, 89(7), 35-36.

Knox, M. and Williamson, M. (2001). The Dynamics of Military Revolution: 1300-2050. New York: Cambridge University Press.

Knox, MacGregor, and Williamson Murray. The Dynamics of Military Revolution: 1300-2050. New York: Cambridge University Press, 2001.

Marine Air-ground Task Force Command and Control, MCWP 3-40.1 W/Chg 1. Washington, DC: Department of the Navy, Headquarters United States Marine Corps, 2003.

Marine Corps Doctrinal Publications MCPD 1. Washington, DC: Department of the Navy, Headquarters United States Marine Corps, 1997.

Marine Corps Doctrinal Publications MCPD 6. Washington, D.C.: Department of the Navy, Headquarters United States Marine Corps, 1996.

Marine Corps Systems Command (2006). D-DACT empowers platoon leaders in Iraq. Marine Corps Systems Command. Retrieved from http://www.marcorsyscom.marines.mil/News/PressReleaseArticleDisplay/tabid/8007/Article/65770/d-dact-empowers-platoon-leaders-in-iraq.aspx

Miller, C. (2012). Making IT Count. Presentation to the Twenty-Fourth Quarterly Symposium of the Small Business and Industry Outreach Initiative. Retrieved from http://www.public.navy.mil/spawar/Atlantic/Documents/Industry/CDCA%204-19-12/CDCA%204-19-12%20Making%20IT%20Count-Miller.pdf

Schneider, K. R. (2008). Tactical communications evolution accelerates. Signal Online. Retrieved from http://www.afcea.org/content/?q=node/1753

Sheehy, C. B. (2000). Tactical network versatility keeps warfighter in touch. Signal, 55(3), 33-36. Retrieved http://www.afcea.org/content/?q=node/240

Skaggs, M. D. (2003). Digital command and control: Cyber leash or maneuver warfare facilitator? Marine Corps Gazette, 87(6), 46-48.

Tsirlis, C. S. (2009). Networking communicates the kill. United States Naval Institute. Retrieved from http://www.mydigitalpublication.com/publication/index.php?i=18623&m=&l=&p=78&pre=&ver=swf

Walker, A. (2011) Army evaluates company command posts at network integration evaluation 12.1. U.S. Army. Retrieved from http://www.army.mil/article/70245/

Walker, A. (2012). Company command posts bring mission command to battlefield edge. U.S. Army. Retrieved from http://www.army.mil/article/82070/